# LAB – 1

**Santhosh Krishna R**

**21BCE1651**

**Aim:** To study about the Burp Suite tool and intercept the connection between system and internet

**Apparatus Required:** Foxy Proxy, Burp Suite

**Apparatus Required: Burp Suite, Foxy Proxy**

## Theory & Commands involved:

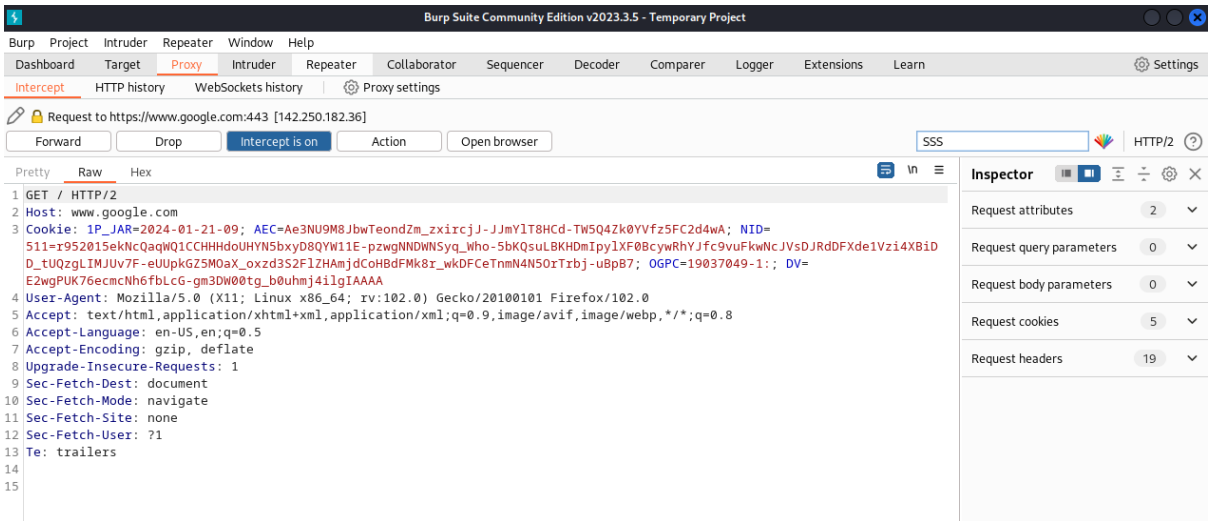
Burp Suite is an integrated platform for performing security testing of web applications.

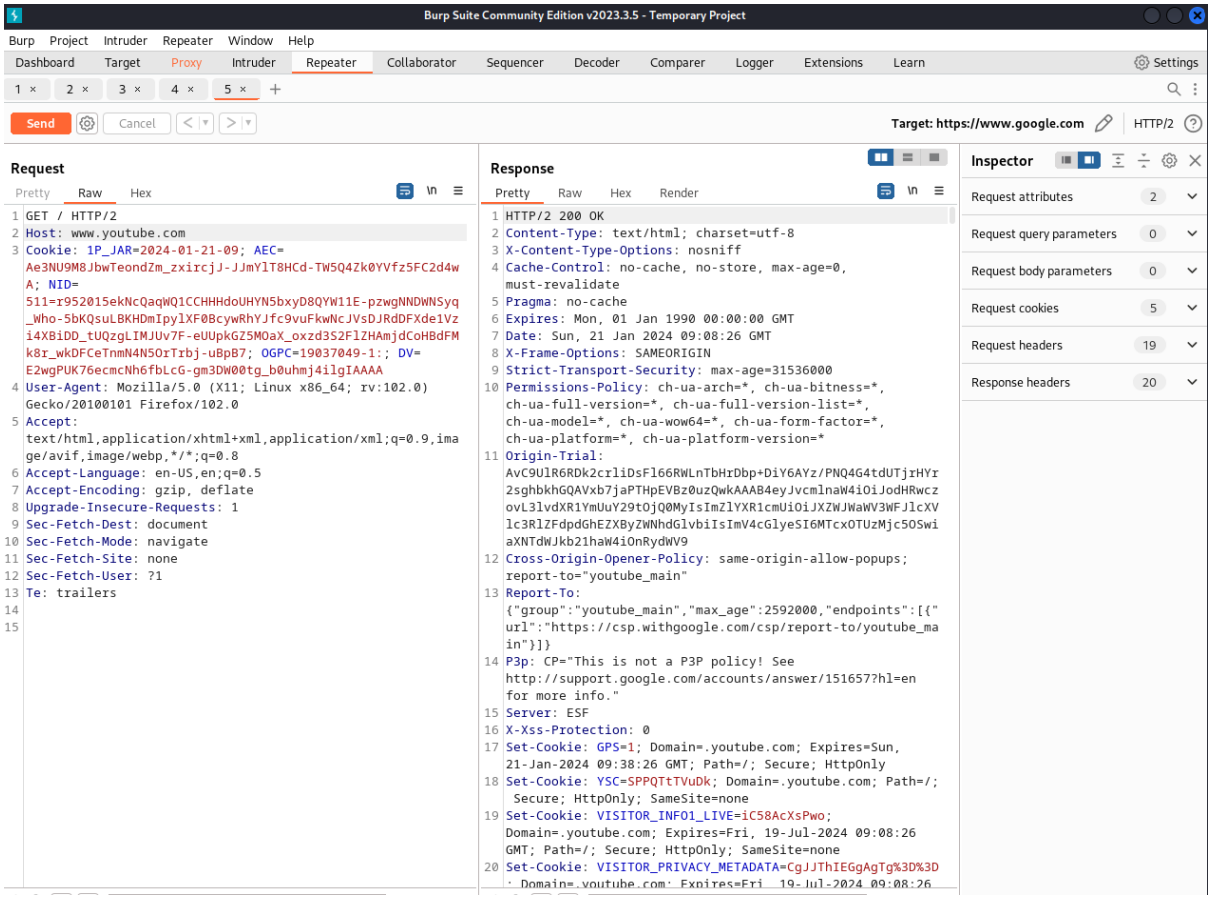
Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

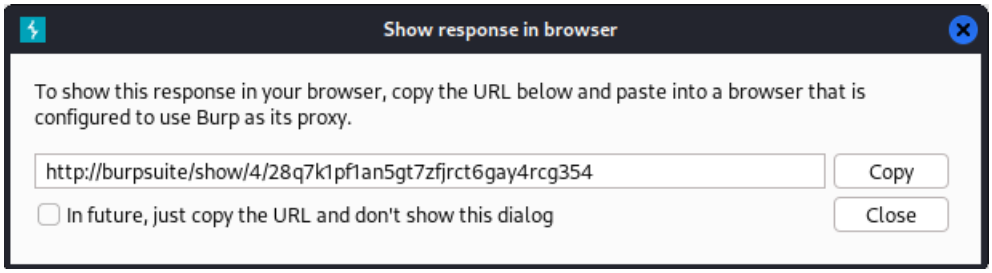
Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

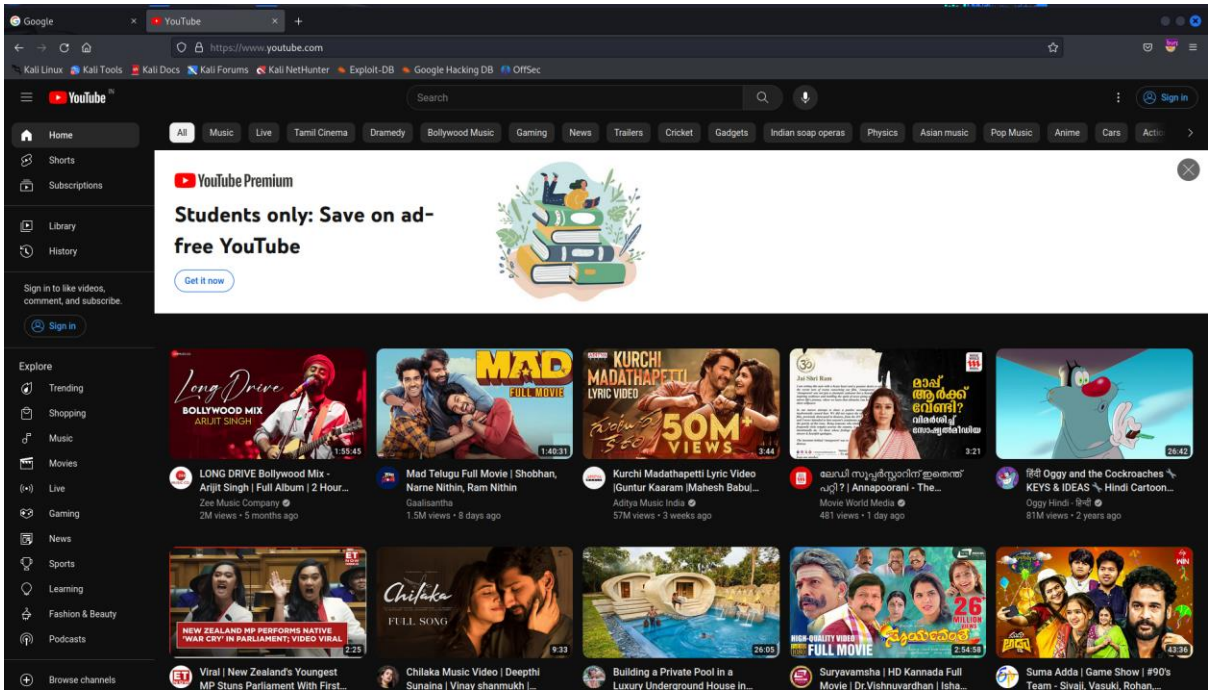
It is the most popular tool among professional web app security researchers and bug bounty hunters.

# Screenshots:






## Conclusion:

Tools offered by Burp Suite

**1. Spider:** It is a web spider/crawler that is used to map the target web application. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found.

**2. Proxy:** BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit.

**3. Intruder:** It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length.

**4. Repeater:** Repeater lets a user send requests repeatedly with manual modifications.

**5. Sequencer:** The sequencer is an entropy checker that checks for the randomness of tokens generated by the webserver. These tokens are generally used for authentication in sensitive operations: cookies and anti-CSRF tokens are examples of such tokens.

**6. Decoder:** Decoder lists the common encoding methods like URL, HTML, Base64, Hex, etc.

This tool comes handy when looking for chunks of data in values of parameters or headers. It is also used for payload construction for various vulnerability classes. It is used to uncover primary cases of IDOR and session hijacking.

**7. Extender:** BurpSuite supports external components to be integrated into the tools suite to enhance its capabilities. These external components are called

**8. Scanner:** The scanner is not available in the community edition. It scans the website automatically for many common vulnerabilities and lists them with information on confidence

over each finding and their complexity of exploitation. It is updated regularly to include new and less known vulnerabilities.

## Results:

Thus, burp suite is installed and its various features are studied.